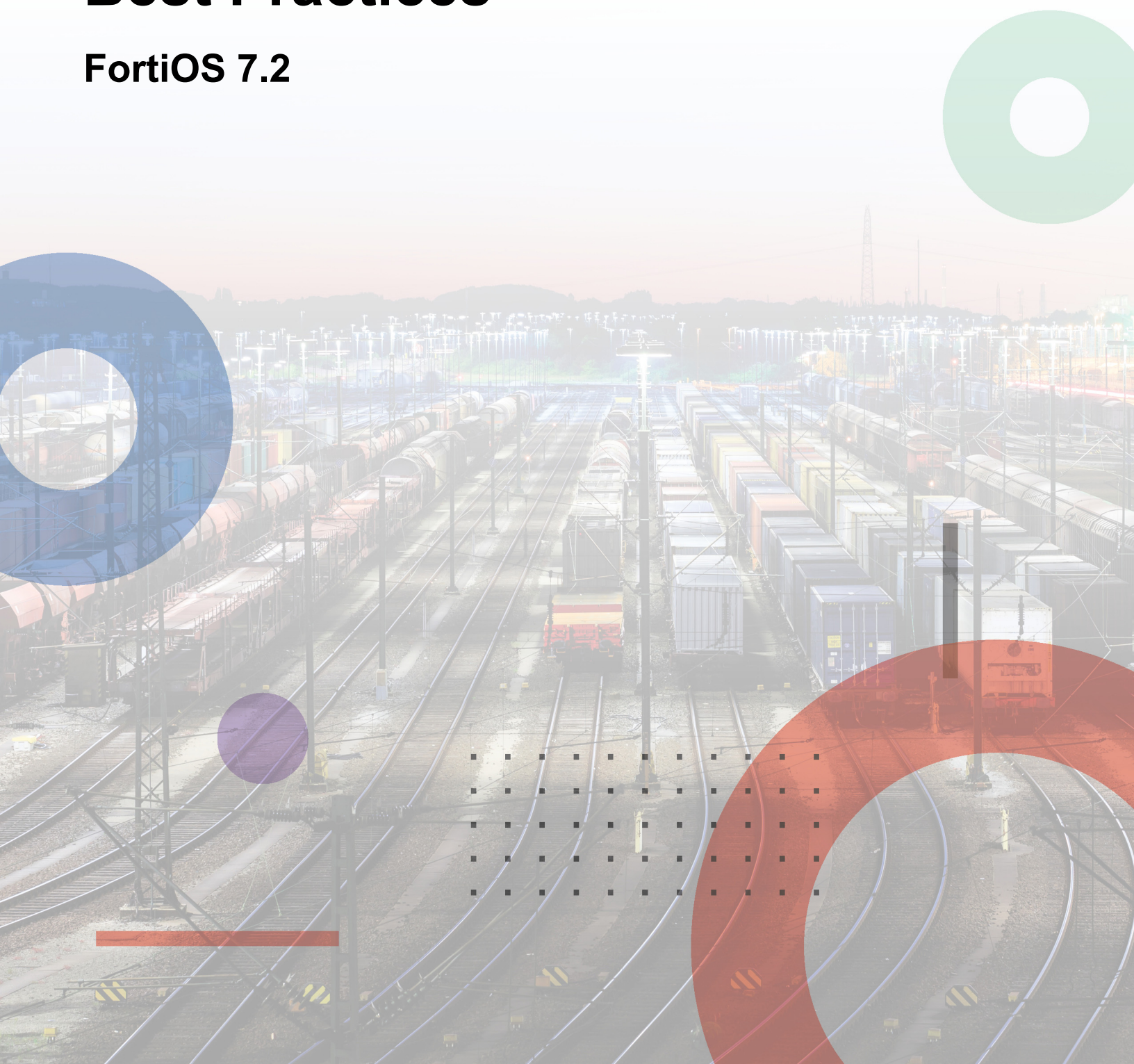
FORTINET

Best Practices

FortiOS 7.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 28, 2023
FortiOS 7.2 Best Practices
01-720-793982-20230928

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-03-31	Initial release.
2022-04-13	Updated Security rating on page 27.
2022-05-18	Updated Hardening on page 35.
2022-05-25	Added Firmware change management on page 40.
2022-07-15	Added Virtual IPs on page 33.
2022-08-22	Updated Security rating on page 27.
2022-10-14	Updated Security profiles on page 17.
2022-10-21	Updated Hardening on page 35.
2023-01-31	Updated Administrative settings on page 10 and Policies on page 32.
2023-03-03	Updated Security profiles on page 17.
2023-05-26	Updated Hardening on page 35.
2023-06-13	Updated Identity and access management on page 14, Certificate usage on page 15, and Encrypted protocols on page 36.
2023-08-25	Added Configuration backup on page 38.
2023-09-18	Updated Hardening on page 35.
2023-09-27	Updated Hardening on page 35.
2023-09-28	Updated Administrative settings on page 10.

Getting started

FortiGate is a complex security device with many configuration options. The following are the first steps to take when preparing a new FortiGate for deployment:

Registration

The FortiGate, and then its service contract, must be registered to have full access to Fortinet Customer Service and Support, and FortiGuard services. The FortiGate can be registered in either the FortiGate GUI or the FortiCloud support portal. The service contract can be registered from the FortiCloud support portal.

To verify the license status on the FortiGate, go to *System* > *FortiGuard* and check the *License Information* table. There can be a delay of a few hours between when you register your device and when the license information on the FortiGate is updated.

The *License Information* table can be used to confirm that the FortiGate is receiving the latest updates. Expand a service in the table and hover over a version to see the day it was last updated. Some services have daily updates, but others will remain unchanged for a longer period of time. For example, the AV engine can stay unchanged for months, while the AV signature database can receive multiple updates a day.

If you are not receiving updates, ensure that the FortiGate's communication with FortiGuard is uninterrupted (see the FortiOS Ports guide), and check the FortiGuard troubleshooting section in the FortiOS Administration Guide.

Basic configuration

As the first step on a new deployment, review default settings such as administrator passwords, certificates for GUI and SSL VPN access, SSH keys, open administrative ports on interfaces, and default firewall policies.

As soon as the FortiGate is connected to the internet it is exposed to external risks, such as unauthorized access, man-in-the-middle attacks, spoofing, DoS attacks, and other malicious activities from malicious actors. Either use the start up wizard or manually reconfigure the default settings to tighten your security from the beginning.

For instructions on connecting to your devices GUI and CLI, see the FortiOS Administration Guide and the FortiGate QuickStart Guides.

- Operating mode:

  NAT mode is preferred for security purposes. NAT mode policies translate addresses in a more secure zone from users that are in a less secure zone using a NATed IP address or IP address pool. This layer of obfuscation prevents malicious actors on the internet from knowing the IP addresses of the resources in your LAN and DMZ.

  Use transparent mode when a network is complex and does not allow for changes in the IP addressing scheme.

- Firmware:

  If the shipped firmware is not the firmware that you will be running, either load the required firmware before doing any configuration, or establish remote access for the additional firmware upload options (SFTP, FTP, SCP, HTTPS) and then load the required firmware.
- Hostname:

  Use a meaningful hostname. It is used in the CLI prompt, as the SNMP system name, as the FortiGate Cloud device name, and as the device name in an HA configuration.
- System time:

  Several FortiGate features rely on an accurate system time, such as logging and certificate related functions. It is recommended that you use a Network Time Protocol (NTP) or Precision Time Protocol (PTP) server to set the system time. If necessary, the system time can be set manually.
- Administrator password:

  The admin administrator password must be set when you first log in to the FortiGate. Ensure that the password is unique and has adequate complexity.
- Management interface:

  Configure the IP address, subnet mask, and only the required administrative access services (such as HTTPS and SSH) on the management interface.

Resources

Fortinet provides many resources to help you configure and use Fortinet devices, software, and services:

Fortinet Document Library https://docs.fortinet.com	Access Fortinet product documentation, including administration guides, reference manuals, release notes, hardware manuals, and QuickStart guides.
Fortinet Video Library https://video.fortinet.com	Become proficient in Fortinet technology with free, learn-as-you-go, videos.
Fortinet Community https://community.fortinet.com	A central repository of technical notes, tips, troubleshooting and debugging, and instructions primarily provided by the technical support team.
FortiGuard Labs https://www.fortiguard.com	Information on the latest internet threats, security advisories, hot bulletins, and malware through the threat encyclopedia. This database has more than four million records and provides access to the signature database. The FortiGuard network resources helps you keep up to date with the security landscape through Advisories & Reports, FortiGuard services, and a Resource library.
Fortinet Blog https://blog.fortinet.com	Read articles and essays about a variety of security related topics.

Customer Service & Support (FortiCloud) https://support.fortinet.com	Start a chat, open a ticket, or call in for immediate service. Be aware of your support SLA with regards to receiving assistance based on the issue severity and Return Merchandise Authorization (RMA) replacement times.
Forti-Companions https://support.fortinet.com/Information/DocumentList.aspx	The Forti-Companion to Technical Support and Forti-Companion to RMA Services documents provide information to help you make the best use of the Technical Support and RMA services.
Professional Services https://www.fortinet.com/support/support-services/professional-services	Assistance with configuring your FortiGate, and other Fortinet products.
Fortinet Training Institute https://training.fortinet.com	Sign up for computer based or instructor led training and hands on labs.

Administrator access

Give special attention to management traffic that is accessing the FortiGate. When access to the FortiGate is insecure, so is the traffic that it passes. The following information can help you prevent unwanted access to your FortiGate:

Management network

There are many benefits to using a management network for administrative access to your network devices:

- Reliability:

  When management traffic is independent from production or business traffic, it does not have to compete for resources and management access can be maintained when reconfiguring the production network.
- Simpler policies:

  Using a management interface allows for policy separation of the management and production traffic. Policies with specific purposes are easier to understand and troubleshoot.
- Security:

  It is more difficult to access network devices on the production network when their management access is on a separate network.

A single interface or VLAN interface in the management network should be dedicated for all administrative access. Administrative access should be disabled on all other interfaces.

Avoid using the WAN interface, or a publicly exposed interface, for management, as it will be subject to constant attacks.

User authentication for management network access

Controlling who can access the FortiGate, and what permission they have, is integral to the security of your network.

Who can access the FortiGate

Users can log in to the FortiGate by authenticating locally with the FortiGate, or with a remote access server that is integrated with the FortiGate, such as LDAP or RADIUS servers.

For local accounts on the FortiGate, define a password policy to ensure a minimum complexity level.

Remote authentication servers enforce their own password policies. They also provide more configuration options. For example, you can use pre-defined security groups to enable access to a group of users. If an administrator's access needs to be removed, when their account is disabled in the remote access server, they are no longer able to log in to the FortiGate.

Do not use shared accounts to access the FortiGate. Shared accounts are more likely to be compromised, are more difficult to maintain as password updates must be disseminated to all users, and make it impossible to audit access to the FortiGate.

In addition to accounts for GUI and CLI administration, the FortiGate can be managed with API calls by API users who are required to generate authorization tokens for REST API messages. If the FortiGate is managed by running scripts over SSH, authenticate users using certificates to avoid storing and maintaining passwords in the application that is making the SSH connection.

What can administrators access

The features that an administrator can access should be limited to the scope of that administrator's work to reduce possible attack vectors. The access profile tied to the user account defines the areas on the FortiGate that the administrator can access, and what they can do in those areas. The list of users with access should be audited regularly to ensure that it is current.

How can users access the FortiGate

Limit access to the FortiGate to a management interface on a management network. Trusted hosts can also be used to specify the IP addresses or subnets that can log in to the FortiGate.

When authenticating to the FortiGate, implement multi-factor authentication (MFA). This makes it significantly more difficult for an attacker to gain access to the FortiGate.

Administrative settings

The following general administrative settings are recommended:

- Set the idle timeout time for administrators to a low value, preferably less that ten minutes.
- Use non-standard HTTPS and SSH ports for administrative access.
- Disable weak encryption protocols.
- Disable the maintainer account if the FortiGate device's physical security cannot be guaranteed.

  The built-in maintainer account is used to log in to the FortiGate if you have lost all administrator credentials. Physical access to the FortiGate device is required. If maintainer account is disabled and you lose all of your administrator credentials, then you will no longer be able to access to access the FortiGate and it will need to be reset to factory default settings.

The maintainer account has been removed in FortiOS 7.2.4 and later.

- Replace the certificate that is offered for HTTPS access with a trusted certificate that has the FQDN or IP address of the FortiGate.
- Configure the Fortinet Security Fabric when multiple FortiGates and fabric devices are used. It provides a single-pane-of-glass administration, allowing administrators access to each device in the fabric using SSO.

  A Fortinet Security Fabric includes a root FortiGate, downstream FortiGates, and other Fortinet fabric devices. A maximum of 35 downstream FortiGates is recommended.

In FortiOS 7.2.6 and later, as part of improvements to reducing memory usage, FortiGate models with 2 GB RAM cannot be the root of the Security Fabric topology or any mid-tier part of the topology. They can only be configured as downstream devices in a Security Fabric or standalone devices.

The affected models are the FortiGate 40F, 60E, and 60F series devices and their variants.

Day to day operations

The two primary reasons to interact with the FortiGate are to make configuration changes, and to check the logs and device performance information.

Configuration changes

Configuration changes on the FortiGate after its initial setup should follow a change procedure as part of your change management plan.

For example, the following is a possible change procedure for changes to the FortiGate configuration:

- Make sure that all of the affected parties are aware of the upcoming change and have a platform to provide input.
- Define the required changes and the objective, to keep the task focused.
- If creating or changing policies, note the following:
  - The purpose of the policy,
  - The affected services, applications, users, and devices,
  - The date that the policy is added and, if applicable, the date that it expires,
  - The name of the person who added or edited the policy.
- Define the possible risks, and plans to mitigate them.
- Define a contingency, or back-out, plan.
- Create a backup of the working configuration before making any changes.
- Prepare a well defined workflow. This can be particularly important if multiple teams are involved.
- Schedule a maintenance window.
- Test the changes, and have them validated by any affected parties.
- Audit and document the completed work.
- Create a backup of the new configuration.

Always maintain a backup of the FortiGate's working configuration. Keeping multiple past configurations is recommended. Backups can be created in the GUI, CLI, and API, and on FortiManager and FortiCloud.

Logging and reporting

Logging generates system event, traffic, user login, and many other types of records that can be used for alerts, analysis, and troubleshooting. The records can be stored locally (data at rest) or remotely (data in motion). Due to the sensitivity of the log data, it is important to encrypt data in motion through the logging transmission channel. Communication with FortiAnalyzer and FortiCloud is encrypted by default. When logging to third party devices, make sure that the channel is secure. If it is not secure, it is recommended that you form a VPN to the remote logging device before transmitting logs to it.

Logging options include FortiAnalyzer, syslog, and a local disk. Logging with syslog only stores the log messages. Logging to FortiAnalyzer stores the logs and provides log analysis . If a security fabric is established, you can create rules to trigger actions based on the logs. For example, sending an email if the FortiGate configuration is changed, or running a CLI script if a host is compromised. If you are using a standalone logging server, integrating an analyzer application or server allows you to parse the raw logs into meaningful data.

FortiSIEM (security information and event management) and FortiSOAR (security orchestration, automation, and response) both aggregate security data from various sources into alerts. The FortiSOAR can also automate responses to different alerts.

Performance monitoring

FortiGate supports multiple protocols for monitoring resource utilization, such as SNMPv3, NetFlow, and sFlow. These protocols are used to measure the performance of the FortiGate and provide insight into the traffic that it is passing.

SNMP polling and traps can be used to optimize monitoring, and the results should be collected and consolidated into meaningful output. A variety of third party SNMP reporting applications can be used to analyze collected results.

Resource monitoring helps to establish resource utilization baselines that can be useful for:

- Configuring IPS signature rates.
- Recognizing abnormal activity, such as when an attack is occurring.
- Comparing the bandwidth utilization over specific time spans, such as month to month or year to year, to plan for growth.
- Comparing the bandwidth utilization between different WANs, and applying SD-WAN and traffic shaping as needed.
- Tuning security profiles to optimize resource usage.

Identity and access management

Secure authentication is paramount in the implementation of an effective security policy. Many of the most damaging security breaches are due to compromised user accounts. By identifying and authenticating users, a significantly more granular control can be implemented to ensure that the right users are accessing the right network resources.

FortiGate supports identifying users in many different ways, including but not limited to:

- Local: The username and password are stored on the FortiGate.
- Remote: The username and password are stored on a remote server, such as LDAPS or TACACS+, that the FortiGate queries.
- PKI/peer: Users that authenticate using a client certificate.

When configuring an LDAP connection to an Active Directory server, an administrator must provide Active Directory user credentials.

- To secure this connection, use LDAPS on both the Active Directory server and FortiGate. See Configuring an LDAP server and Configuring client certificate authentication on the LDAP server.
- Apply the principle of least privilege. For the LDAP regular bind operation, do not use credentials that provide full administrative access to the Windows server when using credentials. See Configuring least privileges for LDAP admin account authentication in Active Directory.

Authentication can be configured for:

- Administrative access
- Firewall authentication and SSO
- VPN
- Wireless security
- 802.1X port security

The most effective authentication includes more than one of the following:

- Something that the user knows: a username and password
- Something that the user has: a certificate, a one time password (OTP) in the form of a token or code either sent to the user over email or SMS, or generated by a hardware token or authenticator app.
- Something specific to the user: biometric data, such as a fingerprint

Single sign-on (SSO) can be used to reduce user fatigue by allowing users to only authenticate one time to gain access to all permitted resources.

FortiClient provides a solution to user and device identification, and can function as an SSO agent. It is also part of the Zero Trust Network Access (ZTNA) solution, allowing security posture checks along with authentication.

Note that, when implementing MFA on the FortiGate, a FortiToken can only be registered to one FortiGate at a time. If you use a remote authentication server for MFA, then each FortiGate points to the server. FortiAuthenticator and FortiToken Cloud are remote authentication servers that can manage the FortiTokens for multiple FortiGates at the same time. This allows you to use one token per user across multiple FortiGates.

Certificates

Certificates serve three primary purposes:

1. Authentication

   The Common Name (CN) and/or Subject Alternative Name (SAN) fields are used to identify the device that the certificate is representing.
2. Encryption and decryption

   Private and public key pairs are used to encrypt and decrypt traffic.
3. Integrity

   Messages are hashed using a secret key known to both the sender and the receiver. The receiver uses the key to check the hash value and confirm the message's data integrity and authenticity.

Certificate based authentication has several advantages over password based authentication. While password based authentication relies on secrets that are defined and managed by a user, certificate based authentication uses secrets that are issued and managed by the certificate authority. Certificates are more secure than passwords, because the private key in the certificate has high cryptographic strength, which a user defined password does not usually have.

The CA vouches for the certificates that it signs. If the endpoint has the CA root certificate installed, then it trusts the CA and anything that the CA signs. There are three types of CAs:

- Public CA

  Public, or well-known, CAs charge a fee to sign your certificate. Many systems come with these CA root certificates pre-installed.
- Let's Encrypt

  Let's Encrypt is a free, automated, and open CA. FortiGate includes an Automated Certificate Management Environment (ACME) to directly interact with Let's Encrypt. Some legacy systems might not have the Let's Encrypt CA root certificate installed.
- Private CA

  Private CAs are created by an organization that creates its own local CA instead of using an external CA. It functions the same as a public CA, but the root certificate is not pre-installed on anything. FortiAuthenticator, Microsoft Server, OpenSSL, and XCA can all function as CAs.

Regardless of what kind of CA is used, involved devices must have the CA root certificate installed in order to trust the certificate that it signs.

Certificate usage

FortiOS leverages certificates in multiple areas, such as administrative access, ZTNA, SAML authentication, LDAPS, VPNs, communication between Fortinet devices and services, deep packet inspection, and authenticating Security Fabric devices.

When configuring an LDAP connection to an Active Directory server, an administrator must provide Active Directory user credentials.

- To secure this connection, use LDAPS on both the Active Directory server and FortiGate. See Configuring an LDAP server and Configuring client certificate authentication on the LDAP server.
- Apply the principle of least privilege. For the LDAP regular bind operation, do not use credentials that provide full administrative access to the Windows server when using credentials. See Configuring least privileges for LDAP admin account authentication in Active Directory.

The default Fortinet factory self-signed certificates are provided to simplify initial installation and testing. Replace any used certificates with certificates that are signed by a trusted CA and specific to that FortiGate

Certificates can be uploaded to the FortiGate in multiple ways:

- Automated Certificate Management Environment (ACME),
- Simple Certificate Enrollment Protocol (SCEP),
- Uploading a certificate in the GUI or CLI,
- Creating a Certificate Signing Request (CSR), having it signed by a CA, then uploading the certificate.

Security profiles

Security profiles define what to inspect in the traffic that the FortiGate is passing. When traffic matches the profile, it is either allowed, blocked, or monitored (allowed and logged).

The protection that a profile provides, and the information that it monitors, can be configured to your requirements, but increased inspection uses more of the FortiGate's resources. Assess your policies' traffic matching, and then apply the necessary level of protection. You might consider implementing denial of service (DoS) security policies to detect and drop illegitimate traffic before it reaches the more resource intensive security profiles (see Denial of service on page 37 for more information).

Security profiles can use flow or proxy mode inspection. Apply flow mode inspection to policies that prioritize traffic throughput, and proxy mode when thoroughness is more important than performance. Under normal traffic conditions, the throughput difference between the two modes is insignificant. For resource optimization, using one mode uniformly across all of the policies is recommended.

Each security profile generates its own log type that contains some log fields that are not present in other logs. This can be important when reviewing or analyzing the logs to assess or troubleshoot user traffic. For example, if no web filtering is applied, then you will not have insight or control of users' browsing information.

The following table lists some basic examples of how a security profile could be used on an edge FortiGate, where inbound traffic goes from the internet to an internal resource using a VIP, and outbound traffic goes from your network to an internet resource:

Security profile	Inbound traffic	Outbound traffic
Antivirus[1]	Protect external resources from malware, such as HTTP PUT requests or FTP uploads.	Scan requested user traffic for malware.
Web filter	Not usually applied to inbound traffic.	Monitor and block user web traffic based on categories and domains.
Video filter	Not usually applied to inbound traffic.	Monitor and restrict YouTube videos based on categories or channels.
DNS filter	Not usually applied to inbound traffic.	Monitor and filter DNS lookups based on domain ratings. Block requests for known compromised domains.
Application control	Make sure that specific protocols are used to access specific ports. For example, only allow SSH traffic to be sent and received over port 22.	Monitor and filter applications on any port.
Intrusion prevention	Protect external services from known exploits and protocol anomalies.	Block connections to botnet sites.
File filter	Prevent uploading files based on the file type and the protocol that is used.	Prevent downloading files based on the file type and the protocol that is used.

Security profile	Inbound traffic	Outbound traffic
Email filter	Perform spam detection and filtering.	Prevent specific IP address or subnets from sending and receiving email messages. Block messages that contain specific words.
Data leak prevention	Prevent sensitive data from entering your network.	Prevent sensitive data, such as credit card numbers or SSNs, from leaving your network.
VoIP	Allow SIP and SCCP traffic, and protect your network from SIP and SCCP based attacks.	Secure clients that are connecting to external SIP servers.
ICAP	Offload tasks to separate, specialized servers.	Offload tasks to separate, specialized servers.
Web application firewall	Detect and block known web application attacks, such as SQL injection, XSS, and known exploits.	Not usually applied to outbound traffic.

[1] Antivirus profiles can submit files to FortiSandbox for further inspection. This enables the detection of zero-day malware, and threat intelligence that is learned from submitted malicious and suspicious files supplements the FortiGate's antivirus database and protection with the Inline Block feature (see Understanding Inline Block feature).

Opened ports for Authentication Override in Web Filter Replacement Messages

When a firewall policy is configured with a web filter, AV or application control, or other UTM security profiles, the policy may open up one or more of ports 8008, 8010, 8015 or 8020 for authentication override and data retrieval for replacement messages, depending on the inspection mode.

When a port is open and you try to access the port on HTTP, this may result in the following behavior:

- FortiGate replies and then redirects to the port with a block message.
- FortiGate sends a TCP RST to close the connection.
- FortiGate doesn't respond.
- FortiGate does a TCP 3-way handshake, then sends a FIN to close the connection.

Traffic does not leak through the policy. However, in some scenarios such as testing the FortiGate for open ports against PCI compliance, this may result in failure of the test case.

To work around the issue, you can close the above ports by doing the following:

```
config webfilter fortiguard
    set close-ports enable
end
```

When `close-ports` is enabled:

- FortiGuard web filter actions *Warning* and *Authenticate* in proxy and flow inspection mode will not work.
- *Allow users to override blocked categories* will not work.
- The replacement message will not display the Fortinet logo.

FortiGuard and Local *URL Filter* blocking will not be affected.

When VDOM is enabled, edit the settings in global:

```
config global
    config webfilter fortiguard
        set close-ports enable
    end
end
```

In the case of Application Control, use the following to disable the use of replacement messages and port 8008:

```
config application list
    edit <list>
        set app-replacemsg disable
    next
end
```

If it is acceptable to simply change the ports to a high ephemeral port, the override ports can be changed from here:

- Default:

  ```
  config webfilter fortiguard
      set ovrd-auth-port-http 8008
      set ovrd-auth-port-https 8010
      set ovrd-auth-port-https-flow 8015
      set ovrd-auth-port-warning 8020
  end
  ```

- Update:

  ```
  config webfilter fortiguard
      set ovrd-auth-port-http <high port>
      set ovrd-auth-port-https <high port>
      set ovrd-auth-port-https-flow <high port>
      set ovrd-auth-port-warning <high port>
  end
  ```

SSL/TLS deep inspection

TLS encryption is used to secure traffic, but the encrypted traffic can be used to get around your network's normal defenses. SSL/TLS deep inspection allows firewalls to inspect traffic even when they are encrypted. When you use deep inspection, the FortiGate serves as the intermediary to connect to the SSL server, then decrypts and inspects the content to find threats and block them. It then re-encrypts the content with a certificate that is signed by the FortiGate, and sends it to the real recipient. The FortiGate acts as a subordinate CA to sign the certificate on the fly, as it re-encrypts traffic. The FortiGate usually uses a subordinate CA certificate that is signed by the company's private CA, such

as a FortiAuthenticator or a Windows server with certificate services. For information about uploading a CA certificate and private key for deep inspection, see Certificates in the FortiOS Administration Guide.

To implement seamless deep inspection, users must trust the certificate that is signed by the FortiGate, and there must be certificate chain back to the trusted root CA that is installed on the user's endpoint. If the root certificate is not installed, the user receives a certificate warning every time they access a website that is scanned by the FortiGate using deep inspection. Administrators should provide the CA certificate to the end users if deep inspection will be used.

Users should be made aware that their communication is subject to these security measures, and that their privacy while protected by a FortiGate that is performing deep inspection cannot be guaranteed. Performing deep inspection might be undesirable when users are accessing certain web categories, such banking or personal health related sites. When creating SSL/SSH inspection profiles that use full SSL inspection, the *Finance and Banking*, *Health and Wellness*, and *Personal Privacy* categories are exempt from inspection by default. Administrators can customize these categories, enable Reputable websites, and add individual addresses to the SSL exemptions as required.

Migration

There are two primary reasons to migrate a FortiGate:

- A FortiGate is been replaced with a different model.
- A different firewall is being replaced with a FortiGate.

The following steps can be used to help with you migration:

1. Audit the current configuration:
   - Remove any unused objects or policies.
   - Analyze the existing policies by assessing traffic flow through the FortiGate and defining what the traffic should look like to determine if any of the policies can be combined.
2. Create diagrams mapping the existing firewall to the new FortiGate.
   For example, port1 on the old firewall could be port2 on the new FortiGate.
3. Configure the general settings first:
   - Interface settings: IP addresses, alias, management access, VLANs
   - Routing: static and dynamic routes
   - HA, if applicable
   - Administrative settings: user account, remove authentication server integration, SNMP, logging, and others
   - Certificates
4. Create the used objects on the FortiGate.
5. Create policies
   - Separate them into sections applicable to your use case and configure them one at a time, for example: by business group (HR, accounting), or by application or service (email, CRM).
6. Create an acceptance test plan:
   - This must be executed as part of the cut-over maintenance window.
   - Have an employee from each affected section verify functionality after the cut-over.
   - If applicable, test HA failover.
7. Verify that the migration worked as planned as far as is possible. A lab that can simulate your normal traffic makes this much easier.
8. Install the new FortiGate during the maintenance window.
   - If possible, install the new FortiGate alongside the existing firewall and only cut-over a small, select group of users.
   - Have a back-up plan in the event that the cut-over does not go as planned.
9. Run user acceptance testing:
   - Have all affected parties ensure that their requirements are unaffected by the change.

Fortinet offers FortiConverter as a one time, paid service that helps migrate configurations to a new FortiGate. It reduces migration complexity, and eliminates common migration configuration errors. For details on purchasing the FortiConverter service, contact you Fortinet sales partner or reseller. After the configuration generated by FortiConverter has been loaded onto the target device, Fortinet technical support or Technical Assistance Center (TAC) can assist with any issues.

Remote access

The number of remote workers is increasing, and networks are expanding into thin branch networks and the cloud. Secure remote access is advancing to meet the requirements of increasingly distributed environments. Assess your requirements and review the available options to determine the solution that best meets your requirements.

Fortinet has IPsec and SSL VPN options. SSL VPN has two modes: tunnel and web.

Regardless of the chosen remote access method, there are several options to enhance the security of the connection:

- Remote authentication servers

  Integrating a remote server for user accounts avoids duplicating accounts on the FortiGate, enabling scalability and reducing human caused errors.
- Certificates

  As a VPN gateway, the FortiGate that you are connecting to can utilize server certificates to prove its identity to the connecting device without requiring confirmation from the end user.

  User certificates can be used in place of passwords. Administrators should assign a unique certificate to each user.
- Multi-factor authentication

  MFA increases the difficulty for an attacker that is trying to establish a connection using a compromised account.
- TLS version and cipher suites

  Setting a minimum TLS version and using high strength cipher suites can enhance security.

SSL VPN

Choosing a mode of operation and applying the proper levels of security depends on your specific environment and requirements.

In tunnel mode, the SSL VPN client encrypts all traffic from the remote client computer and sends it to the FortiGate through an SSL VPN tunnel over the HTTPS link between the user and the FortiGate. It supports a wide range of applications, and provides a transparent user experience when properly configured. FortiClient might enable a DTLS tunnel that allows the SSL VPN to encrypt traffic using TLS, and uses UDP as the transport layer instead of TCP. This avoids retransmission issues that can occur with TCP-inTCP that result in lower throughput. For information on troubleshooting slow SSL VPN throughput, see Troubleshooting common issues in the FortiOS Administration Guide.

Web mode provides clientless network access using a web browser with built-in SSL encryption. It is easier to set up than tunnel mode and does not require that an application be installed on the endpoint, but it has limited application support and requires more resources on the FortiGate.

For more information, see SSL VPN best practices in the FortiOS Administration Guide.

IPsec VPN

IPsec VPN is a standard protocol that allows a variety of solutions for endpoint connectivity, including FortiClient.

It is a well defined protocol that uses specific ports, and it is not uncommon for ISPs to block these ports. On the FortiGate, administrators can configure the ports used for IKE (UDP 500 and 4500) (see Configurable IKE ports). IPsec also has the option to accept a peer ID to specify a tunnel if several tunnels exist on the same interface.

For more information, see IPsec VPNs in the FortiOS Administration Guide.

Non-VPN remote access

In addition to SSL and IPsec VPN, Fortinet offers more advanced solutions for distributed environments:

- Zero Trust Network Access
- FortiSASE SIA

High availability and redundancy

Downtime due to an unexpected network failure negatively impacts business operations. For some companies, some downtime is acceptable; for others, any downtime is unacceptable. Determine your uptime requirements, and ensure that your network has the resilience to meet those requirements.

Building a resilient network costs more initially, as it can include HA, cold standby spares, multiple internet circuits, premium supports contracts, and more.

High availability

HA provides resilience not only in the event of a cluster member failing, but also allows for firmware updates without any downtime. Several HA options are supported by FortiGate: FortiGate Clustering Protocol (FGCP), FortiGate Session Life Support Protocol (FGSP), Virtual Router Redundancy Protocol (VRRP), and auto scaling in cloud environments.

FGCP is the most commonly used HA solution. It allows two or more FortiGates of the same type and model to be put into a cluster in Active-Passive (A-P) or Active-Active (A-A) mode. A-P mode provides redundancy by having one or more FortiGates in hot standby in case the primary device experiences a detectable failure. If a failure occurs, traffic quickly fails over to a secondary device, preventing any significant downtime. A-A mode allows traffic to be balanced across the units in the cluster for scanning purposes, and also performs failover. For FortiGates on the network edge, at least a two unit cluster is recommended.

FGSP is used in more advanced setups that include external load balancers that distribute traffic across the firewall nodes. FGSP members do not need to have the same network configuration, so they do not need to be in the same physical location. Each FGSP member usually has identical firewall policies to enforce the same access rules. Sessions can be failed over from one FGSP member to another if a device failure occurs.

HA is supported on cloud and virtual platforms. In the cloud, HA can be configured in A-P, A-A load balancing, auto-scaling, and others. See the FortiGate Public Cloud documentation for more information.

FortiGates also support VRRP. This can be an appropriate choice when interoperating with third party routers and firewalls. Consult public documentation for further details.

Assess your environment and budget to determine what options are most appropriate for your use case.

Redundant and aggregate links

Using multiple interfaces and links adds resiliency if one link fails, and increases throughput at a lower cost than using a single link with a larger throughput. For example, a 10 GB interface can be less than half the cost of a 20 GB interface.

When using multiple links to connect your FortiGate to the LAN, asses your network for single points of failure. For example, if both links connect to a single switch, and that switch fails, then you could experience an outage. If a single FortiGate is used in the network path, a failure on that FortiGate would also disrupt traffic. A full mesh switching solution along with FortiGate HA could be used so that no single link, switch, or firewall is a point of failure that could disrupt the

entire network. For information on FortiSwitch architectures that can deploy such redundancy, see the FortiSwitch documentation.

SD-WAN

Traffic bottlenecks and disruptions often occur on the WAN links and ISP networks that are outside of your network These can be due to bandwidth limitations, link quality, and other outside factors that are affecting your ISP. Using multiple WAN connections from different vendors can ensure connectivity in the event of an ISP outage and increase performance and throughput. SD-WAN SLA performance health checks can ensure that your WAN connection is always available by selecting the next redundant WAN if the quality of the WAN link is degraded.

SD-WAN can also provide application and service based steering. For example, critical traffic can be steered to a more expensive but more reliable transport link, while less important traffic is steered to a cheaper, higher bandwidth link. After the rules have been defined, traffic steering happens automatically, with failover occurring as needed based on the link health monitors. This can save administrative effort, and the panic caused be network outages, while providing a stable experience for the end users.

For more information about SD-WAN solutions and configurations, see SD-WAN in the FortiOS Administration Guide.

Disaster recovery

It is important to plan what to do in the event that a disaster occurs. Disaster recovery starts with a business continuity plan. This plan should be all-encompassing, and include your FortiGate.

FortiGate disaster recovery should include:

- A tested plan:
  - Without testing the plan, you cannot be sure that it will work.
  - Testing helps to uncover oversights and refine the process.
- Configuration backups:
  - Backups should be made on a schedule, and after any changes have been made to the configuration.
  - It is good practice to evaluate if any unexpected changes occur between backups.
- Remote site assistance:
  - Who will load the configuration backup to the FortiGate?
  - In the event of an RMA, who will install the replacement FortiGate?
  - Do all of the people who will require it have access to the FortiGate?
- Replacement hardware:
  - If the device is covered under warranty, what level of support has been purchased?
  - What is the agreed expectation for a replacement?
  - How will the backup configuration be loaded onto the new device?

After a disaster, review the recovery to asses what worked, what did not work, and what can be improved. Unfortunately, sometimes a disaster helps get approval for a more robust solution, such as HA or a premium support contract with better SLAs.

Security rating

Security audit checks are updated to match evolving vulnerability exploits and attacks. The security fabric rating service helps the security and network teams keep up with changing compliance and regulatory standards by identifying opportunities to improve the system configuration and automate processes. The security rating applies to all devices in your Security Fabric, and uses real-time monitoring to analyze your Security Fabric deployment, identify potential vulnerabilities, highlight best practices that can be used to improve the security and performance of your network, and calculate Security Fabric scores.

The security rating gives grades in the following sections:

- Fabric Security Hardening
- Audit Logging & Monitoring
- Threat & Vulnerability Management
- Network Design & Policies
- Endpoint Management
- Firmware & Subscriptions
- Performance Optimization

The rating also adds consideration for industry standards, such as NIST, PCI DSS compliance, GDPR, and CIS.

Enabling the Security Fabric and rating service allows you to easily identify key deficiencies, take action based on automated recommendations, secure your entire fabric, and passively monitor based on your Security Fabric scores.

The following table lists the security rating tests that are included with FortiOS and do not require a license. The table is grouped by the Score Care category (for example, Security Posture, Fabric Coverage and Optimization) and sorted by the FSBP ID.

Score Card Category	FSBP ID	Name	Description	Category
Security Posture	AL02.1	Centralized Logging & Reporting	Logging and reporting should be done in a centralized place.	Audit Logging & Monitoring
	EM01.1	Endpoint Registration	Interfaces which are classified as "LAN" and are used by a policy should have Security Fabric Connection enabled.	Endpoint Management
	EM01.2	FortiClient Vulnerabilities	All registered FortiClient devices should have no critical vulnerabilities.	Endpoint Management
	ND02.4	FortiAP UTM SSID Compatibility	(blank)	Network Design & Policies
	ND04.1	LAN Segment	Servers should be placed	Network Design &

Score Card Category	FSBP ID	Name	Description	Category
		Servers	behind interfaces classified as "DMZ".	Policies
	ND05.2	VLAN Management	Non-FortiLink interfaces should not have multiple VLANs configured on them.	Network Design & Policies
	ND07.1	Device Discovery	Interfaces which are classified as "LAN" or "DMZ" and are used by a policy should have device detection enabled.	Network Design & Policies
	ND08.1	Interface Classification	All interfaces used by a policy should be classified as either 'LAN', 'WAN', or 'DMZ'.	Network Design & Policies
	ND09.1	Detect Botnet Connections	Policies should block or monitor outgoing connections to botnet sites.	Network Design & Policies
	ND10.1	Explicit Interface Policies	Polices that allow traffic should not be using the "any" interface.	Network Design & Policies
	SH01.1	Unsecure Protocol - Telnet	Interfaces currently in use should not allow TELNET administrative access.	Fabric Security Hardening
	SH01.11	Unsecure Protocol - TFTP	(blank)	Fabric Security Hardening
	SH01.2	Unsecure Protocol - HTTP	Interfaces currently in use should not allow HTTP administrative access.	Fabric Security Hardening
	SH03.1	Valid HTTPS Certificate - Administrative GUI	The administrative GUI should be using a valid and secure certificate.	Fabric Security Hardening
	SH04.1	Valid HTTPS Certificate - SSL-VPN	SSL-VPN should be using a valid and secure certificate.	Fabric Security Hardening
	SH05.1	Admin Password Policy	A password policy should be set up for system administrators.	Fabric Security Hardening

Score Card Category	FSBP ID	Name	Description	Category
	SH09.7	LDAP Server Identity Check	Verify that server-identity-check is enabled for LDAP Servers to ensure certificate validation takes place. While this is the default option in a clean install, it may not be set if upgrading from older releases.	Fabric Security Hardening
	SH09.8	Disable Username Sensitivity Check	Verify that username case sensitivity is disabled for remote LDAP users. This option is provided only for legacy compatibility reasons. If enabled, it can lead to the bypass of two-factor authentication.	Fabric Security Hardening
	SH20.1	DNS Helper	(blank)	Fabric Security Hardening
Fabric Coverage	AL02.2	FortiAnalyzer	All FortiGates in the Security Fabric can connect to and authenticate with their configured FortiAnalyzer.	Audit Logging & Monitoring
	FS01.1	Compatible Firmware	All devices in the Security Fabric should have compatible firmware versions.	Firmware & Subscriptions
	FS01.2	FortiAP Firmware Versions	All FortiAPs should be running the latest firmware.	Firmware & Subscriptions
	FS01.3	FortiSwitch Firmware Versions	All FortiSwitches should be running the latest firmware.	Firmware & Subscriptions
	FS02.1	FortiCare Support	Appropriate devices should be registered with FortiCare and have valid support coverage.	Firmware & Subscriptions
	FS02.10	Firmware & General Updates	Firmware & General Updates subscription should be valid.	Firmware & Subscriptions

Score Card Category	FSBP ID	Name	Description	Category
	FS02.11	Indicators of Compromise	For compromised hosts support the IoC subscription should be valid.	Firmware & Subscriptions
	FS02.2	IPS	IPS subscription should be valid.	Firmware & Subscriptions
	FS02.3	AntiVirus	AntiVirus subscription should be valid.	Firmware & Subscriptions
	FS02.5	Web Filtering	Web Filtering subscription should be valid.	Firmware & Subscriptions
	FS02.6	Anti-Spam	Anti-Spam subscription should be valid.	Firmware & Subscriptions
	FS02.8	Industrial DB	Industrial DB subscription should be valid.	Firmware & Subscriptions
	FS02.9	Outbreak Prevention	Outbreak Prevention subscription should be valid.	Firmware & Subscriptions
	FS03.1	Security Rating	Security Rating subscription should be valid.	Firmware & Subscriptions
	FS05.1	Activate FortiCloud Services	(blank)	Firmware & Subscriptions
	ND01.1	Unauthorized FortiSwitches	All discovered FortiSwitches should be authorized or disabled.	Network Design & Policies
	ND01.2	Unauthorized FortiAPs	All discovered FortiAPs should be authorized or disabled.	Network Design & Policies
	ND06.1	Third Party Router & NAT Devices	No third party router or NAT devices should be detected in the network.	Network Design & Policies
	TV01.1	Advanced Threat Protection	Suspicious files should be submitted to FortiSandbox Appliance/FortiSandbox Cloud for inspection.	Threat & Vulnerability Management
	TV01.2	FortiSandbox	All FortiGates in the Security Fabric can connect to their configured FortiSandbox.	Threat & Vulnerability Management

Score Card Category	FSBP ID	Name	Description	Category
Optimization	ND03.1	Unused Policies	All policies should be used.	Network Design & Policies
	PO01.10	Policy Inspection Mode	Policies should not combine proxy and flow inspection modes.	Performance Optimization
	PO04.1	Managed Switch Capacity Exceeded on FortiGate	Number of managed FortiSwitch should not exceed 80% of the FortiGate's maximum capacity (table size). We suggest upgrading (or adding more FortiGate if the model already has maximum table size) when the threshold is reached.	Performance Optimization
	PO04.2	Redundant FortiLinks	Should have redundant FortiLink between FortiGate and FortiSwitch. We suggest adding FortiLink if there is only 1 FortiLink. Switches not directly connected to FGT are exempt.	Performance Optimization
	PO04.3	Enable MC-LAG	Detect switch peer candidates that can form a tier-1 MC-LAG.	Performance Optimization
	PO04.4	Redundant ISL	Should have redundant inter-switch links between FortiSwitches.	Performance Optimization
	PO04.5	Enable STP	Once the network topology is stable, enable STP on the FortiSwitch ports to avoid a switching loop.	Performance Optimization
	PO04.6	Lockdown LLDP Profile	Edge ports should have LLDP profile locked down to avoid accidental growth in network topology.	Performance Optimization

For more information about security ratings, and details about each of the checks that are performed, go to Security Best Practices & Security Rating Feature.

Network security

Many factors affect how you design your network, the topology that you use, and the placement of your FortiGate in the network, such as:

- The size of your business and the number of users that you are protecting.
- Your business type and industry - service provider, education, healthcare, retail, hospitality, operational technologies, and so on.
- The function or functions that the FortiGate is providing, such as network security, fabric management, multi-cloud security, VPN connectivity, SD-WAN, and so on.
- Who is being protected - employees, customers, students, remote workers, healthcare workers, and so on.
- What is being protected - web servers, office computers, cloud devices, industrial devices, POS terminals, and so on.

For example, a mid-sized retail company might have a corporate headquarters, multiple branches, and physical and cloud-based datacenters, with one or more FortiGates and other Fortinet products deployed at each location.

When designing the network, consider the functionality that you are providing at each location, what you are protecting, and who is allowed access to protected resources. The branches likely have similar or identical setups, and headquarters and the datacenters have setups specific to those locations' requirements. Considering the network design factors helps you define the FortiGate's role (edge firewall, branch firewall, internal segmentation firewall, cloud firewall, and so on), where it is placed in the network, and how to incorporated it and other network solutions into your environment.

The Fortinet solutions page, https://www.fortinet.com/solutions, provides information about products and solutions for different business sizes and industries.

Policies

The FortiGate's primary role is to secure your network and data from external threats. It accomplishes this using policies and security profiles. Policies control what kind of traffic is allowed where, and security profiles define what to look for in the traffic.

FortiGate also has an NGFW mode in which you can allow applications and URL categories directly in the policies, and do not need to define security profiles.

Use the different policy types to secure the different types of traffic that the FortiGate processes.

DoS policies

DoS policies are checked before security policies to prevent attacks from overwhelming your network and FortiGate by triggering more resource intensive security protection. These policies should be adjusted based on your business traffic rates (see Performance monitoring on page 13).

Local-in policies

Local-in policies control access to the FortiGate interfaces. They are often used to block unauthorized access to management ports or other well known ports, and to limit access from specific sources. They should be used to further enable or restrict access to the FortiGate based on your security requirements.

Note that extra care should be taken when configuring a local-in policy, as an incorrect configuration could inadvertently deny traffic for SSL VPN, dynamic routing protocols, HA, and other FortiGate features.

Security policies

- Security policies control the flow of traffic and the security features that are applied to the traffic flow. They are the most commonly used policy type.
- Each policy should have a unique name and there should not be any unused policies.
- Policies that allow traffic should apply to a specific interface, and not the *any* interface.
- Only the security profiles that are necessary for the traffic matching policy should be enabled.
- Security policies are evaluated in order. When traffic matches a policy, further policies are not processed. Put the most specific policies at the top of the list, and follow the least privilege access principle.
- Interface aliases
  - It might not be possible to use the same interface on each FortiGate for the same function. Add aliases to the interfaces so that policies are easier to understand. For example, a policy that controls traffic between you network and your phones switch is clearer if it shows LAN to Phones, instead of port4 to port2.
- Zones
  - Zones are used to group multiple interfaces or subinterfaces into a single interface object that can be used in policies.
  - Grouping interfaces and VLAN subinterfaces into zones simplifies security policy creation by allowing multiple network segments to use the same policy settings and protection profiles.
  - Interfaces in a zone can also still be used individually and still route normally.
- Policies
  - Put the most specific, or narrow, policies at the top of the policy list.
  - Do not use the *all* or *any* objects in a policy, except when routing to the internet.
  - Do not override the implicit deny policy.
  - Use users in policies. This makes the policy more specific and reduces the chances of unintended traffic matching.

Virtual IPs

Policies that include VIPs, or that have `match-vip` enabled, have priority over other policies.

For example, with the following policies, where policy 1 comes first in the list, and policy 2 has a VIP for its destination:

	Policy 1	Policy 2
Source	10.3.3.3	all
Destination	all	WEB_SERVER
Action	deny	accept
Match VIP	disable	n/a

Traffic from 10.3.3.3 to the WEB_SERVER VIP is not blocked, because policy 2 takes priority because it uses a VIP.

If policy 1 is edited to enable `match-vip`, then it will have a higher priority and traffic from 10.3.3.3 to the WEB_SERVER VIP will be blocked.

```
config firewall policy
    edit 1
        set match-vip enable
    next
end
```

Conversely, a VIP could be used in policy 1 to give it higher priority.

The `match-vip` command can only be enabled in deny policies. It is not available in accept policies.

In FortiOS 7.2.4 and later, `match-vip` is enabled by default in new deny policies.

VPN

The following VPNs are for connecting disparate sites to your LAN. See Remote access on page 22 for information about remote user access. There are several was to establish VPN connections between FortiGates, and some that can be applied to other VPN appliances.

OCVPN

OCVPN is a cloud-based solution to simplify IPsec VPN setup. It automatically generates the IPsec configuration, including static routes and policies, on all of the FortiGates in the FortiCare account. It includes self-learning for updates on a FortiGate, such as changing the public IP address in DHCP.

ADVPN

ADVPN is used in hub and spoke topologies. The hub tells two spokes how they can establish a tunnel between each other, instead of routing traffic through the hub.

Site to site

Site to site VPNs are used for a single, secure connection between two sites, or between a site and a cloud service. The connection can be to an external party, such as a contractor or MSSP, or within the same business, such as to connect a remote site to the headquarters.

Hardening

System hardening reduces security risk by eliminating potential attack vectors and shrinking the system's attack surface. Some of the best practices described previously in this document contribute to the hardening of the FortiGate with additional hardening steps listed here.

Physical security

Install the FortiGate in a physically secure location. Physical access to the FortiGate can allow it to be bypassed, or other firmware could be loaded after a manual reboot.

If the FortiGate cannot be physical secured:

- Ensure USB firmware and configuration installation are disabled. They are disabled by default:

```
config system auto-install
    set auto-install-config disable
    set auto-install-image disable
end
```

- Enable port security (802.1x) to prevent unauthorized devices from forwarding traffic.
- Optionally, disable the maintainer account. Note that doing this will make you unable to recover administrator access using a console connection is all of the administrator credentials are lost.

Vulnerability - monitoring PSIRT

Product Security Incident Response Team (PSIRT) continually tests and gathers information about Fortinet hardware and software products, looking for vulnerabilities and weaknesses. The findings are sent to the Fortinet development teams, and serious issues are described, along with protective solutions, in advisories listed at https://www.fortiguard.com/psirt.

Firmware

Keep the FortiOS firmware up to date. The latest patch release has the most fixed bugs and vulnerabilities, and should be the most stable. Firmware is periodically updated to add new features and resolve important issues.

- Read the release notes. The known issues may include issues that affect your business.
- Do not use out of support firmware. Review the Product Life Cycle > Software page and plan to upgrade before the FortiOS End of Support (EOS) date, which is when Fortinet Support services for the firmware version expire.
- Use a federated update to upgrade the firmware of all devices. This process follows the upgrade path to ensure a smooth transition. See Upgrading all device firmware by following the upgrade path (federated update) for more information.
- For standalone FortiGates, enable automatic firmware updates to automatically update firmware based on the FortiGuard upgrade path. The upgrade will only be performed on a patch within the same major release version. See Enabling automatic firmware updates for more information.
- In the event a the user is unable to immediately apply a patch to their device, they have the option to temporarily activate virtual patching within their local-in policies. See Virtual patching on the local-in management interface for more information.

Encrypted protocols

Use encrypted protocols whenever possible, for example:

- LDAPS instead of LDAP
- SNMPv3 instead of SNMP
- SSH instead of telnet
- OSPF MD5 authentication
- SCP instead of FTP or TFTP
- NTP authentication
- Encrypted logging instead of TCP

When configuring an LDAP connection to an Active Directory server, an administrator must provide Active Directory user credentials.

- To secure this connection, use LDAPS on both the Active Directory server and FortiGate. See Configuring an LDAP server and Configuring client certificate authentication on the LDAP server.
- Apply the principle of least privilege. For the LDAP regular bind operation, do not use credentials that provide full administrative access to the Windows server when using credentials. See Configuring least privileges for LDAP admin account authentication in Active Directory.

Strong ciphers

Force higher levels of encryption and strong ciphers. Strong crypto is enabled by default:

```
config system global
    set strong-crypto enable
    set ssl-static-key-ciphers disable
    set dh-params 8192
end
```

See FortiGate encryption algorithm cipher suites for more information.

FortiGuard databases

Ensure that FortiGuard databases, such as AS, IPS, and AV, are updated punctually. Optionally, send an alert if they are out of date.

Penetration testing

Test your FortiGate to try to gain unauthorized access, or hire a penetration testing company to verify your work.

Denial of service

Denial of service (DoS) is a type of attack meant to disable a machine or network causing inaccessibility to the resource or users. Most often this is accomplished by overwhelming the target with more information than it can handle, resulting in a crash. DoS policies, which look for anomalous traffic patterns, are checked before the more resource intensive security policies to help prevent this.

The following guidelines can be used to get started with DoS policies. These policies can be applied to incoming traffic from your local network or internet, depending on your particular network.

- Enable anomaly logging and keep the action as monitor for some time. This is to observe and understand what expected traffic looks like so that you may tune thresholds to have small margins, and therefore more protection. Keep note of false alarms. If they are too frequent, you should adjust your policy accordingly.
- Enable the following DoS policy anomalies to help prevent targeted attacks:
  - tcp_syn_flood
  - tcp_port_scan
  - tcp_src_session
  - tcp_dst_session
  - ip_src_session
  - ip_dst_session

  If you have an idea of your traffic rates for the preceding traffic patterns, you may adjust the threshold. Otherwise, begin with the default and adjust after a period of observing normal traffic. For more information, see DoS protection in the FortiOS Administration Guide.
- Where possible, enable ASIC DoS for offloading using network processor ASICs. The FortiOS Hardware Acceleration Guide contains more information about DoS-related NP6 ASIC features, such as configuring NP6 anomaly protection and using the host protection engine (HPE) to protect the FortiGate from DoS attacks.

Secure password storage

The passwords, and private keys used in certificates, that are stored on the FortiGate are encrypted using a predefined private key, and encoded when displayed in the CLI and configuration file.

Passwords cannot be decrypted without the private key and are not shown anywhere in clear text. The private key is required on other FortiGates to restore the system from a configuration file. In an HA cluster, the same key should be used on all of the units.

To enhance password security, specify a custom private key for the encryption process. This ensures that the key is only known by you.

FortiGate models with a Trusted Platform Module (TPM) can store the master encryption password, which is used to generate the master encryption key, on the TPM. For more information, see Trusted platform module support.

To configure your own private encryption key:

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
********************************
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
********************************
Your private data encryption key is accepted.
```

Configuration backup

The FortiGate configuration file has important information that should always be kept secured, including details about your network, users, credentials, passwords, and keys. There are many reasons to back up your configuration, such as

disaster recovery, preparing for migrating to another device, and troubleshooting. Evaluate the risk involved if your configurations were exposed, and manage your risk accordingly.

When backing up your configuration, consider the following steps to safeguard the file:

- Enable *Encryption* when backing up the configuration.
- Store the configuration file in a secure location.
- Delete old configuration files that are no longer needed.

If a configuration file must be shared with a third party for auditing, troubleshooting, or any other reasons, consider only providing a section of the file and not the entire file. Otherwise, consider the following steps:

- Enable *Encryption* when backing up the configuration and only share the password with the intended party.
- Manually replace the passwords in the backed up configuration file, or enable *Password Masking* when backing up the configuration.
- Request that the configuration file be deleted after the intended purpose has been satisfied.

Firmware change management

Consider the following points when performing firmware upgrades, not only in FortiOS but as general rules for any change you have to make in a production environment.

Understanding the new version

Before attempting any changes in production, first make sure you set up a laboratory where you can freely play with the new features and understand them without pressure and time constraints. Read the release notes, manuals, and other documentation, such as presentations, videos, or podcasts about the new version.

You are ready to explain the need for an upgrade once you understand:

- The differences and enhancements between the new version and the previous versions.
- The impact of the upgrade on customers and the users of the operating platform.
- The known limitations that might affect your environment.
- The potential risks when performing the upgrade.
- The licensing changes that may apply.

Never attempt to upgrade to a version that you do not fully understand, in terms of both features and known limitations, and on which you have no operational experience.

Reasons to upgrade

You should have a valid reason for upgrading the firmware. The reason cannot be only because you want the latest version. The reason has to be explained in terms of business, technical, or operational improvement.

Affirmative answers to the following questions are valid reasons to upgrade:

- Does the new version have a feature that helps to ensure compliance?
- Does the new version have an enhancement that allows a 40% decrease on the time it takes to perform a certain operation?
- Does a new feature correct a known defect or bug found on a previous version that affects the company business or operations?
- Will the new version allow your organization to deploy new services that will help to gain new customers or increase loyalty of existing customers?
- Is the vendor cutting support for the version your organization is currently using?

If the best reason to upgrade is because the new features seem to be cool or because you want the latest version, some more understanding and planning may be necessary.

Preparing an upgrade plan

If you choose to upgrade for a valid reason, make sure you create a plan that covers business, technical, and operational aspects of the upgrade.

Business aspects of the upgrade

Proper planning and justification for an upgrade should be proportional to how critical the system is to the business.

- Make sure you can clearly articulate the benefits of the upgrade in business terms, such as time, money, and efficiency.
- Understand the business processes that will be affected by the change.
- Make sure the upgrade maintenance window is not close to a business-critical process, such as quarterly or monthly business closure.
- Obtain executive and operational approval for the maintenance window. The approval must come from the owners of all the system and information affected by the upgrade, not only from those that own the system being upgraded. The approval must be done formally through written statement or e-mail.

Technical and operational aspects of the upgrade

A plan must be created to account for technical and operational inputs.

- Re-read the release notes for the technology that you are upgrading. Supported hardware models, upgrade paths, and known limitations should be clearly understood.
- Make sure your upgrade maintenance window does not overlap with any other maintenance window on your infrastructure.
- If you have any premium support offer, such as TAM Premium Support, do a capacity planning exercise to ensure the new firmware or software version does not take more hardware resources than you currently have.
- Create a backup, whether or not you already have scheduled backups.
- Obtain offline copies of both the currently installed firmware and the new version.
- Create a list of systems with inter-dependencies to the system you are upgrading. For example, if you are upgrading a FortiGate, understand the impact on any FortiAP, FortiAuthenticator, FortiToken, FortiManager, or FortiAnalyzer you have on your environment.
- If your FortiGate is part of a security fabric, understand any firmware dependencies between fabric devices and plan to upgrade fabric devices as necessary.
- Ensure you have a list of adjacent devices to the upgrading platform and have administrative access to them, in case you need to do some troubleshooting. For example, if you are upgrading FortiWeb, make sure you can administratively access the web applications. Likewise, if you are upgrading FortiGate, make sure you can administratively access the surrounding switches and routers.
- Have a step-by-step plan on how to perform and test the upgrade. You want to make sure you think of the worst situation before it happens, and have predefined courses of action, instead of thinking under pressure when something has already gone wrong.
- Define a set of tests (that include critical business applications that should be working) to make sure the upgrade was successful. If any test does not go well, define which ones mandate a rollback and which ones can be tolerated for further troubleshooting. This set of tests should be run before and after the upgrade to compare results. The

tests performed before and after the upgrade should be the same.

- Define a clear rollback plan. If something goes wrong with the upgrade or the tests, the rollback plan will help you get your environment back to a known and operational status. The plan must clearly state the conditions under which the rollback will be started.
- Declare configuration freezes shortly before and after the upgrade. This reduces the amount of variables to take into consideration if something goes wrong.
- Perform a quality assurance upgrade. Load a copy of the production configuration on a non-production box and execute the upgrade to see if there are any issues on the process. Adjust your plan according to the results you obtain.
- Have a list of information elements to be gathered if something goes wrong. This ensures that, even if the upgrade fails, you will collect enough information to troubleshoot the issue without needing to repeat the problem. Get help from Fortinet Support if you need to confirm what could be missing from your list.
- Define a test monitoring period after the change was completed. Even if the upgrade went smoothly, something could still go wrong. Make sure that you monitor the upgraded system for at least one business cycle. Business cycles may be a week, month, or quarter depending on your organization's business priorities.

Executing the upgrade plan

Execution of an upgrade is just as key as planning. Once you are performing the upgrade, the pressure will rise and stress might peak. This is why you should stick to the plan you created with a cool head.

Resist the temptation to make decisions while performing the upgrade, as your judgment will be clouded by the stress of the moment, even if a new decision seems to be an obvious improvement in the moment. If your plan says you should rollback, then execute the rollback despite the potential quick fix mentality.

While performing the upgrade, make sure all the involved components are permanently monitored before, during, and after the upgrade, either through monitoring systems, SNMP alerts, or with a ping. Critical resources like CPU, memory, network, and disk utilization must also be constantly monitored.

To avoid misunderstandings, when performing the tests for each critical application defined in the planning, make sure there are formal notifications on the results for each user area, service, system, and application tested.

Regardless if you have to rollback or not, if a problem occurs, make sure you gather as much information about the problem as possible, so you can later place a support ticket to find a solution.

Finally, document the upgrade:

- Enable your terminal emulation program to leave trace of all the commands executed and all the output generated. If you are performing steps through the GUI, consider using a video capture tool to document it.
- Document any command or change performed over the adjacent and interdependent systems. Make sure they are acknowledged by the relevant administrators.
- Document any deviations performed over the upgrade plan. This is the planned-versus-actual.

Learning more about change management

Change management and change control are huge knowledge areas in the fields of Information Systems, and Computer and Network Security.

This document is by no means a comprehensive list on what you should do when performing an upgrade, with either Fortinet or any other technology. It is merely a list of important things you should take into consideration when performing upgrades. It is the result of years of experience dealing with changes on critical environments, as it is common that security devices are protecting critical applications and processes.

There are vast resources on the topic of change management and change control, including books, public whitepapers, blog entries, and so on. If you search the internet for the "Change Control Best Practices" or "Change Management Best Practices," you will find many helpful results.

Changes on production IT infrastructure are critical to the business. Make sure they play in your favor and not against you.

For details on upgrading and downgrading your device firmware, see the Fabric Management section of the FortiOS Administration Guide.

www.fortinet.com